UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF NEW YORK	x :	Case No. 1:21-cv-11024-KPF-RWL
- -	:	
UNITED KING FILM DISTRIBUTION LTD, D.B.S. SATELLITE SERVICES (1998) LTD, HOT COMMUNICATION SYSTEMS LTD, CHARLTON LTD, RESHET MEDIA LTD, AND KESHET BROADCASTING LTD, Plaintiffs, -- against -- DOES 1-10, d/b/a **Israel.tv,** Defendants.	: : : : : : : : : : : : : : :	**OPPOSITION OF NON-PARTY CLOUDFLARE, INC. TO PLAINTIFFS' MOTION FOR CONTEMPT**
- -	x	

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

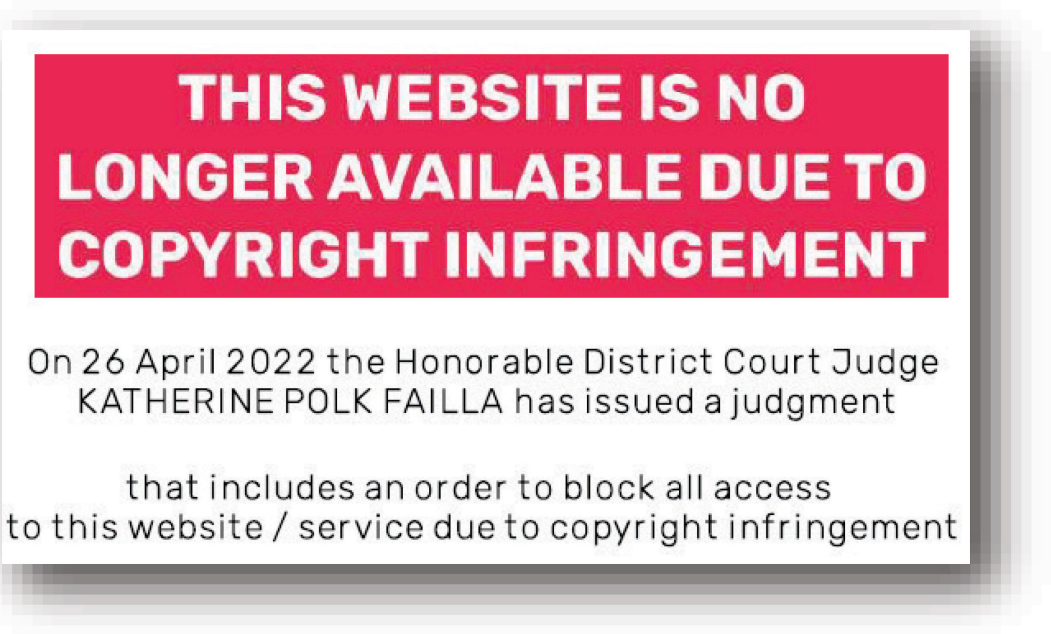
Other Authorities

I. INTRODUCTION

Cloudflare is a leading provider of cybersecurity services to tens of millions of websites. It provides services on a "pass-through" basis—meaning that data passes *through* Cloudflare's network on its way *to* and *from* its customers' websites, but Cloudflare does not, and cannot, control the endpoints of customers using these pass-through services: in particular, among other things, it cannot remove content from these customers' websites. The fact that Plaintiffs filed this "emergency" Motion for Contempt against Cloudflare, and Cloudflare alone, among the dozens of third parties identified in the Injunction in this case, is puzzling.

After obtaining a default judgment against Defendants, Plaintiffs pursued an extremely broad Injunction that purports to bring in a vast number of varied third-party online service providers, including web hosting providers, registrars, registries, and Internet access providers (ISPs). Among that group, Cloudflare is particularly ill-suited to resolve Plaintiffs' concerns, since it does not own or control the websites at issue, cannot remove content from them, and cannot control what appears on them. Cloudflare's obligations under relevant copyright laws and existing court precedent reflect its peripheral position. Yet, despite the fact that their problem regarding the website at issue here has already been resolved, as discussed below, Plaintiffs now seek to control and direct Cloudflare to act outside the scope of the Injunction. Nothing in the law or this Injunction gives Plaintiffs such authority, and their Motion provides no plausible basis for relief.

Plaintiffs' "emergency" Motion is moot now, and was moot before Plaintiffs filed it. As of this writing, the website URL www.Israel.tv (the "Website") redirects a user's browser to a webpage that states:



Declaration of Eric T. Straka ("Straka Decl.") ¶ 2 & Ex. A. Moreover, the relief Plaintiffs' "emergency" Motion seeks was moot even before Plaintiffs filed it: as Plaintiffs could have ascertained if they had simply checked, using well-known and publicly available tools, the Website has not used Cloudflare's services since at least May 26, 2022. There is no further action Cloudflare can take: it cannot withdraw or decline to provide services that Israel.tv is not using. For the same reason, Cloudflare cannot possibly be "in active concert or participation" with Defendants with respect to copyright infringement or other prohibited acts on the Website, when no such acts are occurring. The Court should deny Plaintiffs' Motion as moot on that basis alone.

And the Motion clearly fails to the extent Plaintiffs seek relief with regard to the five domains they identified for the first time in that Motion (the "Add-On Domains"). For the reasons discussed in detail below, *none* of the Add-On Domains are plausibly covered by the Injunction: Plaintiffs fail to provide a shred of evidence, or even any argument, that any of the Add-On Domains are connected to Israel.tv, or that they are owned or operated by Defendants or their

agents.[1] Any reading of the Injunction that attempted to stretch it to cover the Add-On Domains would violate fundamental limitations on the scope of available injunctive relief, including under Federal Rule of Civil Procedure 65(d) and Section 512(j) of the Digital Millennium Copyright Act (17 U.S.C. § 512). Those laws require injunctive relief to be narrowly targeted to specific, identified defendants and their agents, and/or third parties actually in active concert or participation with such defendants. None of those conditions are satisfied here.

Far from seeking relief that is permissible under Federal Rule 65(d) or this Court's rules, Plaintiffs' Motion is a blatant attempt at a power grab. Plaintiffs seek to expand the Injunction to allow them to pick and choose service providers, then force those providers to enforce an overbroad Injunction "against the world" by withdrawing services from *any* third parties Plaintiffs care to identify, *solely* on their say-so and without any due process or judicial oversight, on pain of contempt sanctions. Because Plaintiffs' Motion violates basic legal principles, and flies in the face of the law and the Local Rules, the Court should deny it.[2]

II. BACKGROUND

A. Cloudflare's Security and CDN Services

Cloudflare was founded to protect against the rising threat of malicious cyberattacks online. Like many other third-party services, Cloudflare's security and Content Distribution Network (CDN) services operate between its customers' websites, and users who want to reach those websites. Internet traffic to and from its customers' websites passes through Cloudflare's system, as one link in a chain of transmissions, so that Cloudflare's system can detect and interrupt threats.

[1] As discussed below, to the best of Cloudflare's knowledge, *none* of those domains are owned or operated by Defendants.

[2] At a minimum, because no "emergency" justifies the expedited schedule on which Plaintiffs seek to force Cloudflare to respond, the Court should take the Motion off calendar and order a briefing schedule that will permit the resolution of these issues in an orderly fashion.

Cloudflare both protects its customers (and their users) from attacks, and prevents its customers' websites and online properties from becoming vectors for further attacks.

Before customers can use Cloudflare's services, they must already have a website, a domain name registrar, a web hosting provider, and an ISP to connect the web host service to the Internet—services that Cloudflare has never provided to any of the websites at issue in this Action. In other words, a customer's website must already be up and running online *before* a customer can configure it to send or receive traffic through Cloudflare's network. A customer does so by configuring the website to "point" to Cloudflare's network—a configuration that can only be done by the customer, not by Cloudflare—then substituting a Cloudflare Internet Protocol (IP) address for their web host's IP address. Under this configuration—called a "reverse proxy"—Cloudflare provides security for the customer by "detouring" Internet traffic to and from the customer's website, routing it through Cloudflare's system instead of letting it pass directly to or from the website. This mechanism prevents potential bad actors from directly accessing the customers' servers, gives Cloudflare an opportunity to detect threats before they reach their target, and provides an important safeguard from online attacks. Because applying threat detection to Internet traffic in this manner can make it slower, security services providers have historically sought to compensate by improving Internet performance through other means. Much like other, similar services, Cloudflare does this by operating a content delivery network (CDN), as well as providing other services to help the Internet work faster and more efficiently.

Importantly, Cloudflare cannot remove content from the Internet when websites use its pass-through security and CDN services, because Cloudflare does not host the content in the first place. And while termination of Cloudflare's services to a website may leave the website (and its

users) temporarily more vulnerable to online attacks, it does not remove the website from the Internet, does not interfere with the website's operation, and does nothing to prevent the website from remaining online and accessible. With respect to copyright infringement, in particular, Cloudflare's "pass-through" security, CDN, and other related services are both *unnecessary* to online infringement, and *incapable* of preventing it.

Recognizing that web hosting providers are better positioned to address online abuse, including copyright infringement, Cloudflare operates an abuse reporting system that forwards reports of infringement and other problematic content to both the website's owner and its hosting provider, while also responding to complainants and providing the hosting provider's contact information. A recent federal district court decision—issued after two years of litigation and full discovery of Cloudflare's services and operations—cited Cloudflare's abuse-notification process approvingly in holding that "Cloudflare's performance-improvement services … [and] security services … do not materially contribute to [online copyright] infringement." *Mon Cheri Bridals, LLC v. Cloudflare, Inc.*, 2021 WL 4572015, at *2 (N.D. Cal. Oct. 6, 2021).

B. Procedural History

On or about December 22, 2021, Plaintiffs, six Israeli entertainment and media companies, filed three separate lawsuits against the "Doe" owners and operators of different websites, each of which was purportedly infringing copyrights by streaming motion picture and television content whose copyrights Plaintiffs purportedly owned.[3] Plaintiffs served a document subpoena on

[3] Unless otherwise stated, Cloudflare does not concede the truth of any of Plaintiffs' claims, statements, and allegations in this action, which to Cloudflare's knowledge have never been tested in an adversarial proceeding. For purposes of this response only, Cloudflare does not dispute Plaintiffs' ownership of the copyrights they allege.

Cloudflare, seeking identifying "information regarding the operators and/or owners of the website located at www.Israel.tv … including but not limited to the owners and operators of Isr.dev, Israeltv.to, Israeltv.com and Israeli.tv." ECF 66 (Kaufman Decl.), Ex. C; ECF 68 at 5. Cloudflare responded to acknowledge Plaintiffs' subpoena on March 28, 2022, and shortly thereafter produced documents with identifying information, providing Plaintiffs with "all readily accessible data in [its] possession … responsive to [Plaintiffs'] request[.]" ECF 66 (Kaufman Decl.), Ex. D; ECF 68 at 6; Declaration of Justin Paine ("Paine Decl.") ¶ 2. Cloudflare invited Plaintiffs to contact Cloudflare if they had a need for additional information, but Plaintiffs never requested additional information. Paine Decl. ¶ 2.

On April 26, 2022, the Court granted Plaintiffs' motion for default judgment, ECF 44, and entered a permanent injunction (the "Injunction"), ECF 49, 50. In addition to Defendants and their agents, the Injunction purports to apply to a lengthy list of third party Internet service providers; unidentified domain name "Registrars and Registries"; and "Third Party Services, Generally," which it defines to include virtually every type of online service that Defendants might conceivably use, including hosting providers, ISPs, financial services, and others. *See* Inj. at 7–8.

Plaintiffs served the Injunction[4] on Cloudflare on May 2, 2022.[5] Subsequently, Plaintiffs submitted letters to Cloudflare via email, on May 11, 2022 and May 19, 2022. Mot. at 6; ECF 66 (Kaufman Decl.) ¶ 14 & Ex. H. Both letters demanded that "Cloudflare … cease providing services to the infringing website located at www.Israel.tv." *Id.* Then, on May 24, Plaintiffs filed

[4] For purposes of this Motion only, Cloudflare does not dispute that service was effective.
[5] Plaintiffs' Motion claims, incorrectly, that a copy of the Injunction was served on Cloudflare at its corporate offices in San Francisco on April 29, 2022. Mot. at 8; Kaufman Decl. ¶ 11. The Affidavit of Service states that service was made "[o]n the 2nd day of May, 2022[.]" Kaufman Decl., Ex. E. For purposes of this Response only, Cloudflare does not dispute that service was effective on May 2, 2022.

a letter with this Court requesting that the Injunction be stayed as to the ISPs. ECF 56. Plaintiffs stated that because it was working with the registrars and registries, as well as certain other service providers, they believed it "might not be necessary to enforce the Orders against the ISPs." *Id.*

Two days later, on May 26, 2022, the Website stopped using Cloudflare's authoritative DNS services, as well as its CDN and security services. Paine Decl. ¶ 3. Since then, Cloudflare has not provided any services for the Website. *Id.*

On June 8, 2022, Plaintiffs—notwithstanding that Cloudflare was no longer providing services to the Website, and without having contacted Cloudflare since May 19—filed their Motion,[6] seeking an Order to Show Cause for Expedited Motion for Contempt Against Cloudflare and Alternative Service ("Order to Show Cause"). ECF 58. The Court issued the Order to Show Cause the same day, setting a hearing for June 17, 2022. ECF 69. Although Plaintiffs had been directed to serve Cloudflare by overnight courier on June 9, *see* ECF 69, they sought and were granted leave to serve Cloudflare a day later, *see* ECF 70, 71. At the same time, Plaintiffs also sought to delay the "emergency" hearing on the Order to Show Cause by three days, until June 20; however, the Court denied the request. ECF 70, 71.

Cloudflare received a service copy of the Order to Show Cause on Friday, June 10, 2022.

III. LEGAL STANDARD

An injunction may "only" bind a third party if it is "in active concert or participation with" a party to the litigation or the party's "officers, agents, servants, employees, and attorneys." Fed. R. Civ. P. 65(d)(2)(B), (C). Nonparties may be held in civil contempt for violation of an injunction only if the movant meets its burden to establish that "(1) the order the contemnor failed to comply with is clear and unambiguous, (2) the proof of noncompliance is clear and convincing, and (3) the

[6] For the sake of brevity and clarity, Cloudflare ignores Plaintiffs' multiple misfilings, and Court-ordered re-filings, of what seem to be substantially similar papers. *See* Docket Entries 61-64.

contemnor has not diligently attempted to comply in a reasonable manner." *Next Invs., LLC v. Bank of China*, 12 F.4th 119, 128, 130 (2d Cir. 2021) (internal quotation marks and citation omitted); *Gucci Am., Inc. v. Weixing Li*, 768 F.3d 122, 142 (2d Cir. 2014). The injunction must be "clear and unambiguous… leav[ing] no uncertainty in the minds of those to whom it is addressed, who must be able to ascertain from the four corners of the order precisely what acts are forbidden." *Next Invs.*, 12 F.4th at 131. The moving party must show that the orders "were sufficiently clear to [the third party] *at the time of the alleged conduct*" that "it would not be unreasonable to require compliance in the first instance on pain of contempt." *Id.* (internal quotation marks and citation omitted, emphasis added).

A contempt order is inappropriate "if there is a fair ground of doubt as to the wrongfulness of the alleged contemnor's conduct." *Id.* (internal quotation marks and citations omitted). "Ambiguities in the order's language and persisting questions about legal limits on the court's power can each defeat a contempt motion." *Id.* (citing cases). And, to the extent ambiguities exist, they "should be construed in favor of the person charged with contempt." *Cardell Fin. Corp. v. Suchodolski Assocs., Inc.*, 2012 WL 12932049, at *42 (S.D.N.Y. July 17, 2012); *see A.V. by Versace, Inc. v. Gianni Versace S.p.A.*, 87 F. Supp. 2d 281, 291–92 (S.D.N.Y. 2000) ("[T]he Court must construe any possible ambiguity the preliminary injunction against … the [party] that 'drew the order, chose the language, and presented it to the judge for approval[,]'") (quoting *Gluck v. Camden Fire Ins. Ass'n*, 204 F.2d 183, 185 (2d Cir.1953)).

Civil contempt proceedings may be "commenced [either] by the service of a notice of motion or order to show cause." L.R. 83.6(a). However, "[n]o … order to show cause to bring on a motion[ ] will be granted except upon a clear and specific showing by affidavit of good and sufficient reasons why a procedure other than by notice of motion is necessary[.]" L.R. 6.1(d). "If

the alleged contemnor is found not guilty of the charges, said person shall be discharged from the proceedings and, in the discretion of the Court, may have judgment against the complainant for costs and disbursements and a reasonable counsel fee." L.R. 83.6(d).

IV. ARGUMENT

Plaintiffs have rushed to Court on a spurious "emergency" basis, asking the Court to impose unwarranted contempt sanctions against a single third party, Cloudflare, that has at most an extremely attenuated connection to the Defendants' alleged copyright infringement. Plaintiffs provide no explanation of why, among the dozens of third parties identified in the initial order they pursued—nearly all of them far better able to address Plaintiffs' issues—they chose to seek sanctions against Cloudflare, without prior notice, and based on a flawed, unsupported, factually incorrect theory that Cloudflare failed "to cease providing services to Defendants, as the owners and operators of the website … located at the domain www.Israel.TV[.]" ECF 68 at 12– 13. The relief Plaintiffs seek is unwarranted for multiple reasons that are explained in detail below.

A. The Relief Plaintiffs Seek Is Moot, and Was Already Moot When Plaintiffs Filed Their Motion

Both because the Website is no longer available online, and because Cloudflare had not been providing services to the Website for weeks before Plaintiffs filed their Motion, the relief Plaintiffs seek is moot.

"A civil contempt proceeding is wholly remedial[.]" *United States v. Int'l Union, United Mine Workers of Am.*, 190 F.2d 865, 873 (D.C. Cir. 1951) (collecting cases). In *United Mine Workers*, the court held that civil contempt proceedings brought by the government were moot when its "objectives were accomplished" before a decision was required. *Id.*; *see also Brownlow v. Schwartz*, 261 U.S. 216, 217–18 (1923) (declining to decide issue that had been resolved before the case could be adjudicated, since "[a]n affirmance would ostensibly require something

to be done which had already taken place."); *McLeod v. Loc. 895, United Bhd. of Carpenters, AFL-CIO*, 1970 WL 5416, at *3 (S.D.N.Y. Jan. 13, 1970) (holding that contempt sanction "to enforce compliance [with an injunction] would be essentially an inefficacious exercise" and was "moot," where petitioner sought to stop union members from interfering with moving company's fulfillment of a contract, but the company had "finally satisfied its contractual obligations on the very day … the petitioner came to th[e] court seeking the specified relief.")

Here, Plaintiffs ask the Court to order two measures: first, they seek an order holding Cloudflare in contempt of court "for failing to comply with the Court's Order dated April 26, 2022, which directed Cloudflare to cease providing services to defendant owners and operators of the infringing Website located at www.Israel.tv"; and second, they request an order "[d]irecting Cloudflare to comply with the [Injunction] forthwith[.]" ECF 68 at 13.

But as of this writing—and likely before Plaintiffs filed their Motion—the Website is not publicly available and is inaccessible online. As of this writing, attempting to access the Website redirects the user's web browser to a webpage that provides information about Plaintiffs' litigation, and proclaims that "THIS WEBSITE IS NO LONGER AVAILABLE DUE TO COPYRIGHT INFRINGEMENT." Straka Decl. ¶ 2 & Ex. A.[7] Moreover, the Website stopped using Cloudflare's services (including its CDN, security, and authoritative DNS services) on May 26, 2022, and Cloudflare has not provided such services for the Website since then. Paine Decl. ¶ 3. Simply put, there is no longer anything for Cloudflare to comply *with*: Cloudflare

[7] Cloudflare believes it is highly likely that the Israel.tv Website had been disabled by or at the direction of Plaintiffs before they filed their Motion. But because Plaintiffs failed to notify Cloudflare, and made no attempt to contact Cloudflare before serving the Order to Show Cause, Cloudflare had been unaware that Plaintiffs intended to raise this (non) issue. If Plaintiffs were aware prior to filing their Motion that the Israel.tv Website had been taken down or was no longer accessible online, their failure to disclose that information to the Court is at least disingenuous, if not deliberately misleading.

cannot stop providing services that are not being used, nor withdraw services that it does not provide. Plaintiffs' request that the Court order Cloudflare to "comply … forthwith" with the Injunction seeks a nullity: there is nothing more Cloudflare can do. Nor is there any longer a reason for Plaintiffs to seek this relief because there is nothing left to accomplish.

For the same reasons, it makes no sense for Plaintiffs to seek an order holding Cloudflare in contempt for its supposed failure to "comply" with the Injunction, when for all practical purposes Cloudflare is already doing so. The relief Plaintiffs seek is moot, and their Motion should be denied.

It is unsurprising that Plaintiffs have already achieved their desired result without any need to involve Cloudflare: as a California federal court recently held, "Cloudflare's performance-improvement services … [and] security services … do not materially contribute to [copyright] infringement[.]" *Mon Cheri Bridals,* 2021 WL 4572015, at *2. It follows that withdrawing those services would not prevent infringement. When websites use Cloudflare's pass-through security services, Cloudflare cannot remove content on the websites from the Internet; cannot remove or "disappear" the websites from the Internet; and cannot prevent the websites from remaining fully available online. The types of services Cloudflare provides can be obtained from any number of other providers, so even if Cloudflare were to withdraw its services from a given website at Plaintiffs' behest, that would not affect the infringement either. In contrast, as amply demonstrated by Plaintiffs' success in obtaining control of the Website and effectively removing it and its infringing content from the Internet, other types of service providers *are* necessary to keep a website online, *can* remove content from the Internet, *do* control the web domains of Defendants, and are far better positioned to address Plaintiffs' issues.

B. Cloudflare Cannot Be Held in Contempt on the Basis of the Add-On Domains

The relief Plaintiffs seek in their Motion is explicitly directed to the Israel.tv Website. ECF 65, 66, 68, 69 (seeking a contempt ruling based on Cloudflare's putative provision of services "to Defendants, as the owners and operators of the website … located at the domain www.Israel.TV[,]" and an order "[d]irecting CloudFlare [sic] to comply with the [Injunction] forthwith"). Accordingly, the Motion should be denied for the simple reason that the Website is no longer available online and has not used Cloudflare's service since well before Plaintiffs filed this Motion.

Notwithstanding, and without a clear explanation of their relevance, Plaintiffs also point to five additional websites (the "Add-On Domains") that they identify for the first time in this Motion. Because Plaintiffs have no coherent explanation of why the Add-On Domains provide a basis for contempt proceedings, this Court need not reach them to deny the Motion. Regardless, any motion premised on the Add-On Domains website would fail.

1. The Add-On Domains Are Not Within the Scope of the Injunction

The Injunction's provisions, on their face, do not apply to the five newly identified websites that are neither named in the Injunction, nor connected by any evidence to the Defendants in this action. A careful reading of the Injunction plainly shows that it is focused on, and limited to, *Defendants* and *Defendants'* websites. While the Injunction extends to *Defendants'* agents and to third parties *in active concert* with Defendants, it simply cannot be read to apply to unidentified third parties with no ascertainable connection to Defendants, nor to websites that Plaintiffs think are "like" Defendants' Website. Any reading that purported to bring the Add-On Domains within the ambit of the Injunction would render the Injunction both improperly vague and massively overbroad, and would violate both the general rules governing injunctions under Rule 65, and the

specific rules governing injunctions against online service providers under Section 512(j) of the DMCA.

The Injunction prohibits "Third Party Service Provider[s]" from "providing services used *in connection with Defendants' operations*[.]" Inj. at 7, § II.C (emphasis added). In particular, the Third Party Service Providers are enjoined from "providing services *to the Website* (through any of the domain names set forth in Exhibit A hereto or at any Newly-Detected Websites) or to any *Defendant* in *conjunction with*" the copyright-infringing conduct that *Defendants* are prohibited from engaging in.[8] *Id.* (emphases added). For purpose of the Injunction:

- The defined term *Defendants* means "Defendants Does 1-10, d/b/a Israel.tv, as the owners and operators of the website, service and/or applications … located at or linking to the domain www.Israel.TV[.]" Inj. at 1; *see* Mot. at 4 (defining "Defendants" as "the owners and operators . . . of the web service known as 'Israel.tv'").
- The defined term "Website" means "the Website located at www.israel.tv." Inj. at 26 (Ex. C).[9]

[8] *See id.* at 7, § II.C (enjoining provision of services "in conjunction with any of the acts set forth in subparagraphs (A)(1) to (A)(6) above[.]").

[9] Confusingly, the Injunction elsewhere defines the term "Website" as "the website, service and/or applications (the 'Website') located at or linking to the domain www.Israel.TV[.]" *Id.* at 1. That definition is, on its face, massively overinclusive to the extent it purports to include websites and services that merely "link to" the Israel.tv website: that definition would sweep in every search engine on the Internet—and also the Court's PACER website, where Plaintiffs' Motion includes a live hyperlink to the Israel.tv site. *See* ECF 68 at 13. Plaintiffs also adopt a third definition for purposes of their Motion, namely, "the web service known as 'Israel.tv'[.]" Mot. at 4.

- The defined term "Newly-Detected Websites" is expressly limited to websites at "domain address[es] … to be used in the future *by the Defendants[.]*" *Id.* at 6 (emphasis added).

It is thus clear that the Injunction, to the extent it applies to Cloudflare, prohibits Cloudflare only from providing services *to Defendants* or for specific websites that are "used" *by Defendants*. Plaintiffs provide no evidence to show that any of the Add-On Domains are connected in any way to the Defendants in this action. And to the best of Cloudflare's knowledge after reviewing its records, none of the subscriber information associated with the Add-On Domains matches any of the subscriber information associated with the Israel.tv Website. Paine Decl. ¶ 4.

Perhaps deliberately, Plaintiffs made no effort to obtain identifying subscriber information about the Add-On Domains from Cloudflare before bringing their Motion, despite having been authorized (at their request) to conduct post-judgment discovery, including against Cloudflare. *See* Inj. at 10-12. But in the absence of any subscriber information, or any other evidence linking the Add-On Domains to Defendants in this action, Plaintiffs cannot rest their Motion on conclusory statements that the websites are in some unspecified way "associated with" the Israel.tv Website. Mot. at 6. The mere fact that the domain names are similar proves nothing: anyone can register a domain name. Nor do Plaintiffs offer anything to support their confusing statement that the defunct Israel.tv website is somehow "us[ing] Cloudflare's services through new domains"—whatever that means. *Id.* And nothing in Plaintiffs' Motion or supporting declarations supports Plaintiffs' *non sequitur* statement that by providing services for the Add-On Domains, Cloudflare somehow "enable[s]" the defunct Israel.tv website "to operat[e]," *id.*, particularly when Plaintiffs, having apparently obtained at least practical control of the Website and/or its domain name, must be well aware that it is *not* operating.

In addition to being contrary to any reasonable reading of the injunction (and to common sense), Plaintiffs' claim also is barred by well-established law. As explained further below, Rule 65(d)(1) provides that "[e]very order granting an injunction … must[,]" among other things, "describe *in reasonable detail*… the act or acts restrained or required." (emphasis added). And section 512(j) of the DMCA requires that when an injunction is entered against an online service provider like Cloudflare, it must specifically identify particular content, individuals, or actions. 17 U.S.C. § 512(j)(1), (2). Plaintiffs' attempt to apply the Injunction to websites that the Injunction *does not mention*, based on nothing more than Plaintiffs' unsubstantiated claim that the sites are in some undefined fashion "associated with" the Israel.tv website, plainly violates both Rule 65 and the Copyright Act. Because such a reading is also unsupported by the language of the injunction itself, it should be rejected.

2. In Any Event, Plaintiffs' Failure to Notify Cloudflare of the Add-On Domains Before Filing Their Motion Is Fatal to Their Request for Contempt Sanctions

Even if the Add-On Domains were plausibly within the scope of the Injunction (which they are not), because Plaintiffs failed to provide prior notice to Cloudflare, there is no basis for holding Cloudflare in contempt. A person—and particularly one that is not a party to the underlying litigation—cannot be held in contempt if it did not know what was supposedly required of it.

Plaintiffs' failure to provide previous notice to Cloudflare of domains *that are never mentioned in the Injunction*, then seek sanctions anyway, flies in the face of basic principles of law. Due process requires not only that Plaintiffs provide Cloudflare with notice, but also that Cloudflare have an opportunity to address the issues raised by Plaintiffs' attempt to enforce the Injunction in this unforeseen and unwarranted way. *See, e.g., Golden State Bottling Co., Inc. v. SN.L.R.B.*, 414 U.S. 168, 180 (1973) (finding that "necessary procedural safeguards" to prevent

overbroad application of injunction against third parties was met where "[t]here [would] be no adjudication of liability … without affording [the party] a full opportunity at a hearing, after adequate notice, to present evidence … [and] be heard against the enforcement of any order issued against it.").[10]

C. Sanctions Are Not Warranted Because There Is a "Fair Ground of Doubt" as to the Wrongfulness of Cloudflare's Conduct

A contempt order is inappropriate "if there is a fair ground of doubt as to the wrongfulness of the alleged contemnor's conduct." *Next Invs.*, 12 F.4th at 131 (internal quotation marks and citations omitted). Either "[a]mbiguities in the order's language[,]" or "persisting questions about legal limits on the court's power," "can … defeat a contempt motion." *Id.* (citing cases). Both types of ambiguity are present here, for at least the reasons explained below. In light of the time and space limitations occasioned by Plaintiffs' decision to seek "emergency" review, Cloudflare briefly summarizes the key issues.

1. The Injunction Is Facially Overbroad Under Rule 65

Rule 65(d)(1) provides that "[e]very order granting an injunction … must[,]" among other things, "describe *in reasonable detail*… the act or acts restrained or required." (emphasis added). The Injunction is overbroad and impermissibly vague in a number of respects, including to the extent it purports to apply to "Newly-Detected Websites" that are undefined and unnamed; to the extent it purports to apply to third party service providers "generally" and without reasonable limitation; and to the extent it purports to impose sweeping, indefinite, and perpetual document retention obligations on third parties.

[10] In addition, for the reasons discussed below at § IV.C.3, *infra*, Cloudflare is not in active concert or participation with the owners or operators of the Add-On Domains.

2. The Injunction Is Overbroad Under the Copyright Act

Plaintiffs expressly sought an injunction in this case pursuant to the Section 502 of the Copyright Act, which is the source of the Court's authority to issue an injunction as a remedy for copyright infringement. 17 U.S.C. § 502(a) ("Any court having jurisdiction of a civil action arising under this title may… grant temporary and final injunctions on such terms as it may deem reasonable to prevent or restrain infringement of a copyright."); *see* ECF 35 at 1 (Plaintiffs' motion for injunction). But where—as here—a party seeks to apply an injunction against an online service provider that qualifies for the protections afforded by Section 512 of the Copyright Act, the Court's authority to grant such an injunction is constrained by 17 U.S.C. § 512(j), which sets forth "rules [that] shall apply in the case of any application for an injunction under Section 502 [of the Copyright Act] against a service provider that is not subject to monetary remedies under [§ 512.]"

Cloudflare qualifies for Section 512's limitations on monetary liability—the so-called "DMCA safe harbors"—under one or more of 17 U.S.C. § 512(a), 512(b), 512(c), or 512(d). Each of these subsections shields certain types of online service providers from any monetary liability for copyright infringement, while also strictly limiting injunctive relief against them. With respect to Cloudflare's services that qualify for safe harbor under § 512(a)[11] of the DMCA, any injunction under § 502 that purports to apply to Cloudflare must either:

- *Specifically* identify a Cloudflare subscriber or account holder, and order Cloudflare to terminate that person's account; or
- Order Cloudflare to take *specified* "reasonable steps" to block access to "a specific, identified, online location outside the United States."

[11] By way of example, Cloudflare's "pass-through" services qualify for at least the DMCA's safe harbor for so-called "conduit" service providers under 17 U.S.C. § 512(a).

17 U.S.C. § 512(j)(1)(B)(i), (ii). And with respect to Cloudflare's services that qualify for safe harbor under subsections of the DMCA *other* than § 512(a),[12] any § 502 injunction purporting to apply to Cloudflare must either:

- *Specifically* identify the location of material that Cloudflare is enjoined from providing access to;
- *Specifically* identify an account holder whose account Cloudflare is instructed to terminate; or
- Limit the scope of relief to the "least burdensome" restraint that is "necessary" to prevent infringement of *specific* identified material, at a *specific* online location.

17 U.S.C. § 512(j)(1)(A)(i), (ii), (iii).

3. Cloudflare Is Not in Active Concert or Participation with the Defendants

Rule 65(d)(2) provides that an injunction "binds only the following who receive actual notice of it by personal service or otherwise: (A) the parties; (B) the parties' officers, agents, servants, employees, and attorneys; and (C) other persons who are *in active concert or participation with* anyone described in Rule 65(d)(2)(A) or (B)." (emphasis added).

Cloudflare is not in active concert or participation with customers that sign up for Cloudflare's generally available pass-through and CDN services. As the Federal District Court for the Northern District of California recently held, those services do not materially contribute to online infringement. *Mon Cheri Bridals*, 2021 WL 4572015, at *2. Unlike a number of other types of services—including hosting and registrar services—Cloudflare's pass-through security and CDN services are not necessary to a website remaining online, and Cloudflare has no ability to remove content from the Internet that it does not host. As part of its mission to help make the

[12] By way of example, Cloudflare's CDN service qualifies for, at a minimum, the § 512(a) "conduit" safe harbor, the § 512(b) "caching" safe harbor, and the § 512(c) safe harbor for information residing systems or networks at the direction of users. Cloudflare's DNS service qualifies for the § 512(d) safe harbor for a provider of "information location tools."

Internet more secure, Cloudflare makes its services generally available through its website; its general offer of such "routine" services does not make Cloudflare "substantially intertwined" with "an enjoined party." *Next Invs.*, 12 F.4th at 134 (holding that there was, at a minimum, a "fair ground of doubt" whether a non-party bank's provision of "routine financial services" exposed it to liability under Rule 65(d), *even though* the services "facilitat[ed]" transactions that arguably violated a court's injunctive order) (citing *Nike, Inc. v. Wu*, 2020 WL 257475, at *2 (S.D.N.Y. Jan. 17, 2020)); *accord Nike*, 2020 WL 257475, at *19 (noting that "courts seeking to hold a nonparty liable for contempt on an 'active concert' standard require clear and convincing proof of coordination between the enjoined party and the nonparty").

Rule 65(d) was created "to codify the common-law doctrine that defendants may not nullify a decree by carrying out prohibited acts through aiders and abettors." *Next Invs.*, 12 F. 3th at 134. Cloudflare's provision of routine services that it offers to the general public does not meet this description. Examples of a sufficiently close relationship include "cases where an enjoined party is substantially intertwined with a non-party, including the shared occupation of office space, payment of employee expenses between the non-party and enjoined party, considerable control by the enjoined party over the non-party's operations, and other substantial interconnections." *Nike*, 2020 WL 257475, at *19 (quoting *John Wiley & Sons, Inc. v. Book Dog Books, LLC*, 327 F. Supp. 3d 606, 638 (S.D.N.Y. 2018)). Cloudflare has nothing approaching this type of relationship with its customers.

V. CONCLUSION

The relief Plaintiffs seek is moot: the Israel.tv Website is offline and unavailable, and furthermore, Cloudflare has not provided services to the Website since May 26, 2022, well before Plaintiffs filed their "emergency" Motion. And Plaintiffs have failed to provide any evidence, or even argument, to show that the five Add-On Domains have any connection either to Defendants,

or the Website: as such, the Add-On Domains are not within the scope of the Injunction, obviating any possible argument that Cloudflare should be held in contempt. Contempt sanctions would be unavailable in any event because Plaintiffs failed to provide Cloudflare with notice of those five sites before bringing its Motion. Finally, there are multiple "fair ground[s] of doubt" as to the purported wrongfulness of Cloudflare's conduct, which independently precludes sanctions.

In light of Plaintiffs' apparent failure to reasonably investigate the facts and its failure to notify Cloudflare before bringing this fatally flawed Motion on a needless "emergency" basis, the Court should grant Cloudflare its costs and reasonable attorneys' fees, pursuant to Civil Local Rule 83.6(d), for being required to respond to it.

Dated: June 15, 2022

By: *s/ Thomas J. Kearney*

WINSTON & STRAWN LLP

Jennifer A. Golinveaux (*pro hac vice* pending)
jgolinveaux@winston.com
Thomas J. Kearney (*pro hac vice* pending)
tkearney@winston.com
101 California Street, 35th Floor
San Francisco, CA 94111-5840
Telephone: (415) 591-1000
Facsimile: (415) 591-1400

Attorneys for non-party Respondent Cloudflare, Inc.